e-discovery: revolution or evolution?

December 1st, 2006 marked the implementation of new rules in the United Sates' court procedure to facilitate so-called "e-discovery," requiring the production of electronic data as evidence in civil court cases. As a veteran litigator, John Jennings brings fresh insight into the effect of the "electronic discovery revolution" happening in America.

Although the new rules are few in number, they are collectively referred to by some commentators as a "revolution" because they shift the evidentiary focus of U.S. court proceedings from paper to electronic data. "This taken together with the recent headlines regarding the SWIFT case might lead one to conclude that the U.S. has developed an over ardent zeal for the acquisition of electronic data. However, more careful analysis reveals that e-discovery and other requests for electronic data simply represent established U.S. legal principles adapting to the realities of evolving new technology", says John Jennings.

John Jennings is an accomplished attorney with expertise in international business law, antitrust and competition law, European Union law, bankruptcy litigation and business litigation. He has more than 20 years experience in jury trials as well as in appellate practice in federal circuits, including the U.S. Supreme Court. Before joining Lawfort, he played a leading role in two Kansas City firms where he built an international practice. John Jennings is an author and frequent speaker on EU competition law and U.S. antitrust matters. He has relocated to Belgium for family reasons.

As a veteran litigator, John Jennings brings fresh insight directly from recent major case experience into the effect of the "electronic discovery revolution" (e-discovery) happening in America. "Basically, if you are involved in litigation in the United States, your opponent will have nearly unrestricted access to your e-mails, hard drives, servers, back-up tapes and even your PDA. And while such access is a two-way street – you also have access to your opponent's electronic data – the burdens of dealing with and reviewing this electronic information are daunting and the costs can be extremely high."

What is e-discovery?

Jennings: "I think it's easier to start with the word 'discovery' which if you are not a lawyer probably doesn't make a lot of sense in itself. In American civil proceedings – criminal and civil are completely separate in the United States - because the jury system is much more facts and documents oriented in terms of evidence, the parties have the opportunity to ask each other questions in writing which have to be answered under oath, ask each other for documents and to talk each other's witnesses also under oath and in front of a court reporter. That phase is called 'discovery'. And that is not new: that's been around for 70 years. But what is new is that in the last 10 years people started asking for emails and electronic documents such as Word, Excel and PDF files, and that area of discovery has grown to the extent that in my opinion it is now more significant than the old "normal" area of discovery. Companies can find themselves in very difficult circumstances, for instance if the opposing party requests all e-mails and you are a big company that would potentially be thousands of gigabytes of information. And someone has to go through it all >

> The new rules offer a 'safe harbor' provision that did not exist in the past with respect to electronic data that was innocently lost or destroyed. This provision actually protects companies from sanctions when data destruction is the result of the routine, good-faith operation of their electronic information system.

to determine what's relevant, what's not, what's privileged, and what's not. It's enormously time consuming and expensive. That is e-discovery or electronic discovery."

Impact of e-discovery in the U.S on the European companies

If you are, for instance, a Belgian company with no business operation outside of Belgium and nothing going on in the US, this is probably of general interest but not urgent for you to understand. But a lot of Belgian companies are now international and are doing business in the United States including some which have branch offices or a sales force in the US and thus subject to the jurisdiction of American courts. So those companies are going to have to be alert to this and be prepared for it just as any American company has to be aware of it and be ready to deal with it in the event of litigation.

"Once involved in litigation in the U.S., European companies are of course subject to U.S. rules of procedure. Under U.S. civil procedure, the parties, or more accurately their attorneys, have the power to conduct investigations into the facts. With the development of widespread computerization, U.S. attorneys began asking opponents not only for paper documents but also documents that might exist only in electronic format, such as e-mails. In recent years the preference has shifted from paper documents to requests for electronic documents, not only e-mails but word processing files, spreadsheets and PDFs found on hard drives, servers, back-up tapes and the like. These novel developments were treated by the courts with deliberation and the law in this area grew incrementally by analogy to existing rules."

Once litigation hits, you have the absolute duty to stop destroying data and that includes automatic overwriting. So if your server is updating itself every night and overwriting deleted files, you may have to stop that once your are involved in a U.S. court procedure. Many companies have found to their distress that is not easy – although it sounds easy because you can call your IT department and say 'You better stop'. But if you have multiple servers and multiple locations it's very difficult to comply and it is more or less on an emergency basis so to be prepared is to be aware of this in advance.

"Of course, the financial world is not exempt. In addition, in the United States of course we have Sarbanes-Oxley with its record-keeping requirements. There is also the Graham-Leach-Bliley Act which is a privacy act regarding financial institutions' obligations with respect to the maintenance and protection of personal private data. So you have a legal duty to keep and protect some records while on the other hand you may be dealing with the difficulties of complying with electronic discovery requests. So for banking and financial services, in addition to e-discovery, there are many data-related compliance issues which can be quite complex." >

▲ *John Jennings: 'All these record-keeping requirements that now include electronic records, balanced on the other hand with the potential to get involved in litigation and have e-discovery requests and comply with e-discovery, and add another layer if you are a European company you have to comply with the data protection directive, I think that electronic compliance has to be more than an afterthought.'*

E-DISCOVERY

The amendments to the Federal Rules of Civil Procedure on the discovery of electronically stored information (e-discovery) cover five areas:

- the definition of discoverable material;
- the early attention to issues relating to e-discovery, including the format of production;
- the discovery of electronically stored information from sources that are not reasonably accessible;
- the procedure for asserting claim of privilege or work product protection after production;
- a "safe harbor" limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems (www.uscourts.gov)

How long should information be kept?

On the e-discovery side, there is no stated time period. It has to be reasonable and based on good faith. It can be done on a business necessity basis, for instance.
The Federal Rules of Civil Procedure were amended on December 1st of 2006 to implement e-discovery. In the amendment it is said that if electronic documents are destroyed in good faith pursuant to regular records keeping practise, for instance everything over 5 years is simply deleted and we never see it again, a party cannot be sanctioned for failure of not still having that document. It does not say 'five years,' but a 'routine, good-faith system'.

On the other side, Sarbanes-Oxley, the Graham-Leach-Bliley Act, the U.S. Tax Code, and Securities and Exchange Commission Rules, all do have stated periods of years to retain such data.

Being unprepared can be very costly

Companies that are involved in litigation in the U.S. have a duty to preserve documents and data that they know or should have reason to know may be used as or related to evidence in a trial. And that is a very tricky standard because how and when are you supposed to know? In the US, the rule is when you knew or reasonably should have known that you are going get sued for firing this person or for breaching this contract, that you have a duty to preserve all evidence and related documents including, as mentioned before, stopping your electronic system from automatically overwriting and deleting documents.

Secondly, if you do get involved in litigation and someone asks for these documents, you'll have to produce the relevant documents which typically means going into all your documents to figure out which documents are relevant.

Thirdly, there is a possibility in special circumstances that you will have to restore a back up tape or retrieve archived data.
And last but not least, don't forget that a company could face very significant fines and sanctions if found in violation of these rules. This was, for instance, the situation with Arthur Andersen in the Enron case.
Also in 2006, Morgan Stanley & Co. Inc. agreed to pay a $15 million civil fine to settle federal regulators' charges that it repeatedly failed to provide tens of thousands of e-mails that the government sought in major investigations over the years. Another interesting case was Zubulake versus UBS Warburg LLC. Zubulake, a female employee, sued her employer UBS Warburg for sex discrimination and failure to promote. Several UBS employees allegedly deleted e-mails relevant to Zubulake's claims, and several backup tapes that contained these and other relevant e-mails were missing. As a result, a number of e-mails containing relevant information were irretrievably lost, while others were produced after the close of discovery. As a sanction, the court ordered UBS to pay Zubulake's attorneys' fees and expenses relating to the issues. Judgment against UBS was ultimately $29.2 million, due to e-mail evidence and the court's sanctioning instructions to the jury.

> Electronic compliance has to be more than an afterthought. It really has to move up on the list of corporate priorities in order to avoid finding yourself unprepared at some crucial point.

Most of European companies are not aware of the situation

Jennings: "I think that most of European companies are not aware of the situation and I suppose I am being a little bit of an evangelist to promote this and sound the warning bell. I would say that most European lawyers don't know too much about e-discovery and I assume for their clients, banks and insurance companies it's the same.

Generally speaking of bank and financial institutions, between Sarbanes-Oxley, Basel II, USA Patriot Act, etc..., all these record-keeping requirements that now include electronic records, balanced on the other hand with the potential to get involved in litigation and have e-discovery requests and comply with e-discovery, and add another layer if you are a European company you have to comply with the data protection directive, I think that electronic compliance has to be more than an afterthought. It really has to move up on the list of corporate priorities in order to avoid finding yourself unprepared at some crucial point."